

UNITED STATES DISTRICT COURT

for the
Western District of WashingtonIn the Matter of the Search of)
Information associated with One Target)
Telephone, for Investigation of 21 U.S.C.)
§§ 841, 846, and Other Offenses)

Case No. MJ20-501

APPLICATION FOR A SEARCH WARRANT AND PEN-TRAP ORDER

I, Adam Roeser, a federal law enforcement officer or an attorney for the government, request a search warrant and pen-trap order, and state under penalty of perjury that I have reason to believe that on the person or property described in Attachment A, located in the Western District of Washington, there is now concealed property and evidence described in Attachment B. This Court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☐ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 841, 846


Offense Description
Possession with Intent to Distribute Controlled
Substances, Conspiracy

The application is based on the facts set forth in the attached affidavit, which is incorporated herein by reference with all attachments and exhibits. Pursuant to 18 U.S.C. § 3123(a)(1), Exhibit 1 to the affidavit includes a certification from an attorney from the government that the requested information is relevant to an ongoing criminal investigation.

- ☒ Delayed notice of 90 days (give exact ending date if more than 30 days: November 1, 2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 41, this warrant is presented by:

- ☒ by reliable electronic means; or ☐ telephonically recorded


Applicant's signature

Adam Roeser, FBI Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn before me and signed in my presence, or
☒ The above-named officer provided a sworn statement attesting to the truth or the foregoing affidavit by telephone.

Date: August 4, 2020


*Judge's signature*City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO #2020R00703

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT AND PEN-TRAP ORDER

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I, Adam Roeser, a Special Agent with the Federal Bureau of Investigation, Seattle, Washington, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an Application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **(310) 918-2928**, with listed subscriber name of “DAMON E SMITH” (“SMITH”), billing address of “2218 S 134TH ST, SEATAC, WA 98168,” and service provided by AT&T with a service start date of May 4, 2017 (hereinafter referred to as the **Target Cell Phone**). The **Target Cell Phone** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

ECPA

2. The Court has jurisdiction to issue the proposed warrant under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2713, because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

Pen Register Act

3. Because this warrant seeks the prospective collection of information that falls within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to comply with the Pen Register Act, 18 U.S.C. §§ 3121-3127.

1 4. The Court has jurisdiction to issue the requested pen-trap order because it is
2 a “court of competent jurisdiction” under 18 U.S.C. § 3122(a)(2). Specifically, the Court
3 is a district court of the United States that “has jurisdiction over the offense being
4 investigated.” 18 U.S.C. § 3127(2)(A)(i).

5 5. This application includes all the information required by the Pen Register
6 Act. *See* 18 U.S.C. §§ 3122(b) & 3123(a)(1). Namely, Exhibit 1 to this application is a
7 certification from Assistant United States Attorney Cecelia Y. Gregson that (1) identifies
8 the Federal Bureau of Investigation and Drug Enforcement Administration as the law
9 enforcement agencies conducting the investigation and (2) certifies the information likely
10 to be obtained is relevant to an ongoing criminal investigation being conducted by that
11 agency. 18 U.S.C. § 3122(b). The Assistant United States Attorney is an “attorney for
12 the government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

13 6. A “pen register” is “a device or process which records or decodes dialing,
14 routing, addressing, or signaling information transmitted by an instrument or facility from
15 which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3). A “trap
16 and trace device” is “a device or process which captures the incoming electronic or other
17 impulses which identify the originating number or other dialing, routing, addressing, and
18 signaling information reasonably likely to identify the source of a wire or electronic
19 communication.” 18 U.S.C. § 3127(4).

20 7. In the traditional telephone context, pen registers captured the destination
21 phone numbers of outgoing calls, while trap and trace devices captured the phone
22 numbers of incoming calls. Similar principles apply to other kinds of wire and electronic
23 communications such as emails, text messages, connection logs, and data transfers. The
24 prospective location data sought in this application constitutes “dialing, routing,
25 addressing, and signaling information” covered by the Pen Register Act. Accordingly,
26 the requested warrant will record, decode, and/or capture dialing, routing, addressing, and
27 signaling information associated with the Target Cell Phone without geographic limit.
28

12. On or about June 12, 2020 in the Central District of California, SMITH was charged in an under-seal indictment in case number CR No. 2:20-CR-00221-FMO with violating 21 U.S.C. Section 846 (conspiracy to distribute and possess with intent to distribute controlled substances); and 21 U.S.C. Section 841 (possession with intent to distribute controlled substances). An arrest warrant for SMITH was also issued on June 12, 2020, commanding that SMITH be arrested to answer for the charges in the Indictment. Because the Indictment involves eight defendants in total and to avoid possible flight from prosecution and destruction of evidence (stemming from piecemeal arrests), the agents plan to arrest them in a coordinated takedown, currently anticipated for August 2020.

13. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting SMITH, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

STATEMENT OF PROBABLE CAUSE

14. The United States, including the FBI and DEA, is conducting a criminal investigation of SMITH regarding violations of 21 U.S.C. Section 846 (conspiracy to distribute and possess with intent to distribute controlled substances); and 21 U.S.C. Section 841 (possession with intent to distribute controlled substances).

15. On July 13, 2020, agents queried law enforcement databases, including but not limited to California Department of Motor Vehicle (“CA DMV”), Washington Department of Motor Vehicle (“WA DMV”), CLEAR, and Accurant, and learned the following regarding the **Target Cell Phone**, believed to be used by SMITH:

//

//

//

1 a. In July 2020, an administrative subpoena was served to AT&T
2 requesting the subscriber of the **Target Cell Phone**. AT&T subpoena results revealed
3 that starting in May 2017, the **Target Cell Phone** was subscribed to “DAMON E
4 SMITH.”

5 b. The subscriber address for the **Target Cell Phone** was “2218 S
6 134TH ST, SEATAC, WA 98168.” One of the current owners of the residence is listed as
7 Aleczandria Jamerson. Based on the investigation of SMITH, I understand that
8 Aleczandria Jamerson and SMITH have multiple children together.

9 c. The subscriber address listed for the **Target Cell Phone** is also the
10 address listed on an expired Washington driver license belonging to SMITH, expired as
11 of June 8, 2020.

12 d. According to the WA DMV, SMITH’s driver’s license was renewed
13 on May 18, 2020 and expires on June 8, 2026, which lists an address of “13345 MARTIN
14 LUTHER KING JR WAY S APT R107 SEATTLE WA 98178-5209.”

15 e. Starting in February 2020, the **Target Cell Phone** was associated
16 with SMITH through commonly used law enforcement databases such as Accurant, and it
17 showed that his social security number ending in 7935, was also associated to the
18 number.

19 f. The **Target Cell Phone** has a California area code and the user of
20 the **Target Cell Phone**, SMITH, is believed to spend time between California and
21 Washington. The Central District of California, the charging District, currently has a
22 warrant authorizing the “(1) The Disclosure of GPS and Cell-Site Information and (2)
23 Use of Cell-Site Simulator and Request to Seal,” signed by United States Magistrate
24 Judge, Honorable Steve Kim, and served to AT&T on or about July 14, 2020.

25
26 //

27
28 //

1 16. As of July 29, 2020, the results of the warrant obtained in the Central
2 District of California indicate that the **Target Cell Phone** is located in the Seattle,
3 Washington area. The results of the GPS locate have regularly been over 3000 meters,
4 which is unhelpful because it can cover multiple city blocks over a two mile area in a
5 densely populated region.

6 17. Because SMITH lists the **Target Cell Phone** in his name, is associated
7 with the **Target Cell Phone** through multiple law enforcement databases, and has
8 multiple addresses associated with his identity (which law enforcement is still
9 investigating), I believe there is probable cause to grant disclosure of prospective cell-site
10 and trap and trace information relating to the **Target Cell Phone** to assist in located
11 SMITH.

12 18. I seek prospective cell-site and trap and trace information via this
13 application because this information will assist in locating and apprehending SMITH.
14 Given the vast coverage area of the existing GPS locates and the training and experience
15 of myself and other technically trained law enforcement officers, I feel obtaining the
16 prospective cell-site and trap and trace in this district will aid in detecting a more precise
17 location of the **Target Cell Phone**. Moreover, it will assist in targeting surveillance and
18 reduce risk of being prematurely detected before SMITH is in custody. Fugitives, as well
19 as people who are involved in criminal activity, are often conscious of being followed
20 and keep a close eye out for surveillance units. The chance of being discovered increases
21 with the more surveillance that is done and the closer the surveillance units must get to
22 their target subject. Use of prospective cell-site and trap and trace information enables the
23 investigative team to be more focused and judicious in its use of surveillance and enables
24 the investigative team the ability to conduct surveillance at a greater distance, because the
25 fear of losing the target is reduced when surveillance is maintained via prospective cell-
26 site and trap and trace information.

27 19. Based on my training and experience, I know each cellular device has one
28 or more unique identifiers embedded inside it. Depending on the cellular network and

1 the device, the embedded unique identifiers for a cellular device could take several
2 different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic
3 Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber
4 Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network
5 Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an
6 International Mobile Equipment Identity (“IMEI”). The unique identifiers -- as
7 transmitted from a cellular device to a cellular antenna or tower -- can be recorded by
8 pen-traps and indicate the identity of the cellular device making the communication
9 without revealing the communication’s content.

10 20. Based on my training and experience, I know that when a cell phone
11 connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the
12 cellular antenna or tower, and the cellular antenna or tower records those identifiers as a
13 matter of course. The unique identifiers -- as transmitted from a cell phone to a cellular
14 antenna or tower -- are like the telephone number of an incoming call. They can be
15 recorded by pen-trap devices and indicate the identity of the cell phone device making the
16 communication without revealing the communication’s content. In addition, a list of
17 incoming and outgoing telephone numbers is generated when a cell phone is used to
18 make or receive calls, or to send or receive text messages (which may include
19 photographs, videos, and other data). These telephone numbers can be recorded by pen-
20 trap devices and then used to identify the parties to a communication without revealing
21 the communication’s contents.

22 21. Based my training and experience, I know that a cell phone can also be
23 used to exchange text messages with email accounts. The email addresses associated
24 with those text messages can be recorded by pen-trap devices and then used to identify
25 parties to a communication without revealing the communication’s contents.

26 22. Based on my training and experience, I know that cellular phones can
27 connect to the internet via a cellular network. When connecting through a cellular
28 network, internet communications sent and received by the cellular phone each contain

1 the same unique identifier that identifies cellular voice communications, such as an ESN,
2 MEIN, MIN, SIM, IMSI, MSISDN, or IMEI. Internet communications from a cellular
3 phone also contain the IP address associated with that cellular phone at the time of the
4 communication. Each of these unique identifiers can be used to identify parties to a
5 communication without revealing the communication's contents.

6 23. In my training and experience, I have learned that AT&T is a company that
7 provides cellular telephone access to the general public. I also know that certain
8 providers of cellular telephone service have technical capabilities that allow them to
9 collect and generate information about the locations of the cellular telephones to which
10 they provide service, including cell-site data, also known as "tower/face information" or
11 cell tower/sector records. Cell-site data identifies the cell towers (i.e., antenna towers
12 covering specific geographic areas) that received a radio signal from the cellular
13 telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the
14 telephone connected. These towers are often a half-mile or more apart, even in urban
15 areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to
16 a wireless device does not necessarily serve every call made to or from that device.

17 24. When using a cellular connection to receive or transmit data, a cellular
18 phone typically utilizes a cell tower to make telephone calls, send or receive text
19 messages, send or receive emails, surf the internet, carry out application-initiated data
20 transfers, among other things.

21 25. Based on my training and experience, I know that AT&T can collect cell-
22 site data about the Target Cell Phone. Based on my training and experience, I know that
23 for each communication (including data connections) a cellular device makes, its wireless
24 service provider can typically determine: (1) the date and time of the communication; (2)
25 the telephone numbers involved, if any; (3) the cell tower to which the customer
26 connected at the beginning of the communication; (4) the cell tower to which the
27 customer connected at the end of the communication; and (5) the duration of the
28 communication. I also know that wireless providers such as AT&T typically collect and

1 retain cell-site data pertaining to cellular devices to which they provide service in their
2 normal course of business in order to use this information for various business-related
3 purposes.

4 26. Different service providers use different systems, applications, and reports
5 to collect or analyze cell site data. These systems, applications, and reports are referred
6 to by a variety of names including, but not limited to real-time tool or “RTT” (Verizon),
7 Periodic Location Updates or “PLU” (Verizon), per call measurement data or “PCMD”
8 (Sprint), Network Event Location System or “NELOS” (AT&T), EVDO, ALULTE,
9 Timing Advance, and TruCall. RTT data, for example, estimates the approximate
10 distance of the cellular device from a cellular tower based upon the speed with which
11 signals travel between the device and the tower. This information can be used to estimate
12 an approximate location range that is more precise than typical cell-site data.

13 27. Based on my training and experience, I know that wireless providers such
14 as AT&T typically collect and retain information about their subscribers in their normal
15 course of business. This information can include basic personal information about the
16 subscriber, such as name and address, and the method(s) of payment (such as credit card
17 account number) provided by the subscriber to pay for wireless communication service. I
18 also know that wireless providers such as AT&T typically collect and retain information
19 about their subscribers’ use of the wireless service, such as records about calls or other
20 communications sent or received by a particular device and other transactional records, in
21 their normal course of business. In my training and experience, this information may
22 constitute evidence of the crimes under investigation because the information can be used
23 to identify the Target Cell Phone’s user or users and may assist in the identification of co-
24 conspirators and/or victims

25 28. Modern cell phones allow users to switch their telephone numbers, use
26 multiple telephone numbers on a single device, and transfer their telephone number to a
27 different cell phone. These changes can be made with the assistance of the wireless
28 provider or by taking actions such as changing the “SIM card” (short for “subscriber

identity module card”) of a cellphone. To provide for any such changes made to the Target Cell Phone, Attachment A specifies that the property to be searched includes: (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number assigned to an instrument now bearing the same unique identifying number (such as an IMSI, ESN, MSID, or IMEI) as the telephone number listed above, or that was bearing the same unique identifying number as the telephone number listed above, at any point within the last 30 days, (iii) any changed unique identifying number subsequently assigned to the same telephone number, or (iv) any additional changed telephone number and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone numbers listed above, within the period of disclosure authorized by this warrant.

AUTHORIZATION REQUEST

29. Based on the foregoing, I request that the Court issue the proposed search warrant and pen-trap order, pursuant to Federal Rule of Criminal Procedure 41, 18 U.S.C. § 2703(c), and 18 U.S.C. § 3123.

30. I further request that the Court direct AT&T to disclose to the government any information described in Attachment B that is within the possession, custody, or control of AT&T. I also request that the Court direct AT&T to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with AT&T’s services. The agency shall reasonably compensate AT&T for reasonable expenses incurred in furnishing such facilities or assistance.

31. Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant by serving the warrant on AT&T. Because the warrant will be served on AT&T, who will then compile the requested records and data, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I therefore request that

1 the Court authorize execution of the warrant at any time of day or night, owing to the
2 potential need to locate the **Target Cell Phone** outside of daytime hours.

3 **REQUEST FOR DELAYED NOTICE**

4 32. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of
5 Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to
6 delay notice to the subscriber or user of **Target Cell Phone** until 90 days after the
7 collection authorized by the warrant has been completed. There is reasonable cause to
8 believe that providing immediate notification of the warrant may have an adverse result,
9 as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of
10 **Target Cell Phone** would seriously jeopardize the ongoing investigation, as such a
11 disclosure would give that person an opportunity to destroy evidence, change patterns of
12 behavior, notify confederates, and flee from prosecution, especially if SMITH were to
13 learn that he had already been indicted in a federal case for drug-trafficking offenses. *See*
14 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into
15 the warrant, the proposed search warrant does not authorize the seizure of any tangible
16 property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant
17 authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C.
18 § 2510) or any stored wire or electronic information, there is reasonable necessity for the
19 seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

20 //

21 //

22 //

REQUEST FOR SEALING

33. I further request that the Court order that all papers in support of this Application, including the Affidavit, Search Warrant, and Pen/Trap Order, and all related documents, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.



Adam Roeser, Affiant
Special Agent
FBI

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 4th day of August, 2020.



MARY ALICE THEILER
United States Magistrate Judge

EXHIBIT 1

DECLARATION

I, Adam Roeser declare as follows:

1. I am a duly appointed Assistant United States Attorney for the Western District of Washington, and I have primary responsibility for representing the interests of the United States herein.

2. I make this declaration in support of an application for a search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) with an integrated pen-trap order pursuant to 18 U.S.C. §§ 3122 and 3123.

3. Pursuant to 18 U.S.C. § 3122(b), I certify that the FBI and DEA are the law enforcement agencies conducting the investigation in this matter and that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by that agency.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing Application is made on the basis of information officially furnished, and on that basis I verily believe such information to be true.

Executed this ____ day of August, 2020.

s/ Cecelia Y. Gregson

CECELIA Y. GREGSON

Assistant United States Attorney

ATTACHMENT A**Property to Be Searched and Subscriber/Subject Information**

1. Records and information associated with the cellular phone assigned call number (310) 918-2928, with listed subscriber "DAMON E SMITH" (the "**Target Cell Phone**"), that is in the custody or control of AT&T, a company headquartered at 208 Akard St., Dallas, TX 75202. The subscriber of the **Target Cell Phone** is Damon E. SMITH. The identity of the person who is the subject of the criminal investigation is believed to be Damon E. SMITH.

2. The property to be searched includes: (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number assigned to an instrument now bearing the same unique identifying number (such as an IMSI, ESN, MSID, or IMEI) as the telephone number listed above, or that was bearing the same unique identifying number as the telephone number listed above, at any point within the last 30 days, (iii) any changed unique identifying number subsequently assigned to the same telephone number, or (iv) any additional changed telephone number and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone numbers listed above, within the period of disclosure authorized by this warrant.

ATTACHMENT B**Particular Things to be Seized**

This warrant is issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2713, and the Pen Register Act, 18 U.S.C. §§ 3121-3127. As such, this warrant authorizes the collection of subscriber records, pen-trap data, and cell site data information regarding the **Target Cell Phone**. **This warrant does not authorize the disclosure or seizure of any tangible property or the content of any wire or electronic communication, as defined in 18 U.S.C. § 2510(8).** Accordingly, the Court finds reasonable necessity for the seizure of the data and records identified below. *See* 18 U.S.C. § 3103a(b)(2).

I. Information to be Disclosed by AT&T

1. **Subscriber/Account Information for Target Cell Phone.** The following non-content information about the customers or subscribers associated with the Account listed in Attachment A:

- a. Names (including subscriber names, user names, and screen names);
- b. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- c. Local and long distance telephone connection records for two billing cycles;
- d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions for two billing cycles);
- e. Length of service (including start date) and types of service utilized;
- f. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Number (“MIN”),

Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

g. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and

h. Means and source of payment for such service (including any credit card or bank account number) and billing records.

2. Pen Register/ Trap and Trace Data and Associated Subscriber Records to Be Provided for a Period of no more than 45 Days for Target Cell Phone.

a. AT&T shall install and monitor pen-trap devices to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the **Target Cell Phone** including the date, time, and duration of the communication, and the following, without geographic limit and without notice to the subscriber:

(i) IP addresses associated with the cell phone device or devices used to send or receive electronic communications;

(ii) Any unique identifiers associated with the cell phone device or devices used to make and receive calls with the cell phone number described in Attachment A, or to send or receive other electronic communications, including the ESN, MEIN, IMSI, IMEI, SIM, MSISDN, or MIN;

(iii) IP addresses of any websites or other servers to which the cell phone device or devices connected; and

(iv) Source and destination telephone numbers and email addresses.

b. On a 24-hour-a-day basis, for the duration of the authorized pen-trap devices, AT&T shall provide the following records for those subscribers whose identifiers are obtained pursuant to the use of the pen-trap devices: published or non-published subscriber names and addresses, including billing addresses.

1 **3. Prospective Cell Site Location Information for Target Cell Phone.**

2 a. All information about the location of the **Target Cell Phone**
 3 described in Attachment A for **a period of 45 days**, during all times of day and night.
 4 This information includes: precise location information, as well as all data about which
 5 “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e.,
 6 faces of the towers) received a radio signal from the cellular telephone(s) or account(s)
 7 described in Attachment A.

8 b. The physical address and coverage maps of cell towers used by the
 9 **Target Cell Phone.**

10 To the extent that the cell site information described in the previous paragraphs
 11 (hereinafter, “Location Information”) is within the possession, custody, or control of
 12 AT&T, AT&T is required to disclose the Location Information to the government
 13 pursuant to this warrant. In addition, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-
 14 (b), AT&T must furnish the government all information, facilities, and technical
 15 assistance necessary to accomplish the collection of the Location Information
 16 unobtrusively and with a minimum of interference with AT&T’s services. The
 17 government shall compensate AT&T for reasonable expenses incurred in furnishing such
 18 facilities or assistance.

19
 20
 21 **II. Information to Be Seized by the Government**

22 1. All information described above in Section I that will assist in arresting
 23 Damon E. SMITH, who was charged with violating 21 U.S.C. Section 846 (conspiracy to
 24 distribute and possess with intent to distribute controlled substances); and 21 U.S.C.
 25 Section 841 (possession with intent to distribute controlled substances) on June 12, 2020,
 26 is the subject of an arrest warrant issued on June 12, 2020, and is a “person to be
 27 arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).
 28

1 2. All non-content subscriber/account information provided pursuant to 18
2 U.S.C. § 2703(c) regarding the **Target Cell Phone**.

3 3. All non-content dialing, routing, addressing, and signaling information
4 provided pursuant to 18 U.S.C. §§ 3121-3127 regarding the **Target Cell Phone**.

5 4. Location Information regarding the **Target Cell Phone**.

6 Law enforcement personnel (who may include, in addition to law enforcement
7 officers and agents, attorneys for the government, attorney support staff, agency
8 personnel assisting the government in this investigation, and outside technical experts
9 under government control) are authorized to review the records produced by AT&T in
10 order to locate the things particularly described in this Warrant.